Notice of Allowability	Application No.	Applicant(s)	
	09/828,559	SHIBATA ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *response filed on 11/17/2009, and additional amendments proposed on 2/25/209*.

2. ☒ The allowed claim(s) is/are *1,3-14,16-26,28,31-37,39 and 42-50*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *2/25/2009* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Farid Homayounmehr Examiner Art Unit: 2439	/Kambiz Zand/ Supervisory Patent Examiner, Art Unit 2434

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/17/2008 has been entered.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Howard Sobelman on 2/25/2009.

The application has been amended as follows.

In the claims:

1. (Currently Amended) A copyright protection system comprising:

an encryption device and a decryption device, wherein cryptographic communication is performed between the encryption device and the decryption device using a contents encryption key and a contents decryption key,

wherein the encryption device includes

a contents storage section for storing contents,

a first contents key generation section for generating the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation, and

a first encryption section for encrypting the contents using the contents encryption key and outputting the encrypted contents, and

wherein the decryption device includes

a second contents key generation section for generating the contents decryption key from the second decryption limitation, the second decryption limitation obtained by updating the first decryption limitation in the decryption device, and

a first decryption section for decrypting the encrypted contents transferred from the encryption device using the contents decryption key generated by the second contents key generation section, and

wherein the encryption device further includes a third encryption section for encrypting the first decryption limitation using a time-varying key and outputting a

second encrypted decryption limitation to the decryption device, and the decryption device further includes a third decryption section for decrypting the second encrypted decryption limitation transferred from the third encryption section using the time-varying key and outputting the first decryption limitation, and

wherein the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

a second encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation, and

the encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation,

wherein the time-varying key is not required to be transmitted to the decryption device; and

wherein the first contents key generation section generates the contents encryption key based on the second decryption limitation generated by the second decryption section.

2. (Cancelled)

3. (currently amended) A copyright protection system according to claim 1 ~~2~~, wherein the encryption device further includes

a first common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, and

a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and

wherein the decryption device further includes

a second common key storage section for storing the common key,

a second random number generation section for generating the second random number,

a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, and

a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section.

4. (Currently Amended) A copyright protection system according to claim 1,

~~wherein the encryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and~~

~~a second contents key generation section for generating the contents decryption key based on the second decryption limitation updated by the first decryption limitation updating section~~,

wherein the encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section,

the first contents key generation section generates the contents encryption key based on the second decryption limitation updated by the first decryption limitation updating section.

5. (previously presented) A copyright protection system according to claim 4, wherein the encryption device further includes

a first common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, and

a first time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, wherein the time-varying key is not required to be transmitted to the decryption device, and

wherein the decryption device further includes

a second common key storage section for storing the common key,

a second random number generation section for generating the second random number,

a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, and

a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section.

6. (original) A copyright protection system according to claim 5,

wherein the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance,

the first contents key generation section generates the contents key from the second decryption limitation, and

the second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

7. (original) A copyright protection system according to claim 3,

wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key.

8. (previously presented) A copyright protection system according to claim 3,

wherein the first and second contents key generation sections generate the contents encryption key and the contents decryption key based on the second decryption limitation and the time-varying key.

9. (previously presented) A copyright protection system according to claim 3,

wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence

key based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key.

10. (previously presented) A copyright protection system according to claim 3,

wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key.

11. (previously presented) A copyright protection system according to claim 3,

wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second contents key generation sections generate the respective contents encryption key and contents decryption key based on the second decryption limitation and the respective data sequence key.

12. (previously presented) A copyright protection system according to claim 3,

wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and

wherein the first and second contents key generation section generate the respective contents encryption key and contents decryption key based on the second decryption limitation, the time-varying key, and the respective data sequence key.

13. (previously presented) A copyright protection system according to claim 3,

wherein the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol.

14. (Currently Amended) An encryption device for performing cryptographic communication in association with a decryption device using a contents encryption key, comprising:

~~a contents storage section for storing contents;~~

~~a second encryption section for encrypting the first decryption limitation using a time-varying key and outputting a second encrypted decryption limitation to the decryption device, without transmitting the time-varying key to the decryption device;~~

~~a contents key generation section for generating the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation; and~~

~~a first encryption section for encrypting the contents using the contents encryption key and outputting the encrypted contents,~~

a contents storage section for storing contents;

a first contents key generation section for generating the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation;

a first encryption section for encrypting the contents using the contents encryption key and outputting the encrypted contents; and

a third encryption section for encrypting the first decryption limitation using a time-varying key and outputting a second encrypted decryption limitation to the decryption device;

a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation,

wherein cryptographic communication is performed between the encryption device and the decryption device using the contents encryption key and a contents decryption key,

wherein the decryption device includes

a second contents key generation section for generating the contents decryption key from the second decryption limitation, the second decryption limitation obtained by updating the first decryption limitation in the decryption device;

a first decryption section for decrypting the encrypted contents transferred from the encryption device using the contents decryption key generated by the second contents key generation section;

a third decryption section for decrypting the second encrypted decryption limitation transferred from the third encryption section using the time-varying key and outputting the first decryption limitation;

a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

a second encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation, and

wherein the time-varying key is not required to be transmitted to the decryption device; and

wherein the first contents key generation section generates the contents encryption key based on the second decryption limitation generated by the second decryption section.

15. (Cancelled)

16. (previously presented) An encryption device according to claim 14, further including

a common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, and

a time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section.

17. (previously presented) An encryption device according to claim 14, further including a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule in response to the updating of a decryption limitation by the decryption device,

wherein the contents key generation section generates the contents encryption key based on the second decryption limitation obtained by the decryption limitation updating section.

18. (previously presented) An encryption device according to claim 17, further including

a common key storage section for storing a common key,

a decryption limitation storage section for storing the first decryption limitation,

a first random number generation section for generating a first random number,

a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, and

a time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section.

19. (previously presented) An encryption device according to claim 17, wherein:

the decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance;

the decryption limitation updating section outputs the second decryption limitation to the contents key generation section;

the contents key generation section generates the contents encryption key from the second decryption limitation; and

the decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

20. (original) An encryption device according to claim 16, wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

21. (previously presented) An encryption device according to claim 16, wherein the contents key generation section generates the contents encryption key based on the second decryption limitation and the time-varying key.

22. (original) An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device, the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

23. (original) An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

24. (previously presented) An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the contents key generation section generates the contents encryption key based on the second decryption limitation and the data sequence key.

25. (previously presented) An encryption device according to claim 16, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device,

wherein the contents key generation section generates the contents encryption key based on the second decryption limitation, the time-varying key, and the data sequence key.

26. (Currently Amended) A decryption device for performing cryptographic communication in association with an encryption device using a contents decryption key, comprising:

~~a second decryption section for decrypting a second encrypted decryption limitation transferred from the encryption device using a time-varying key and outputting a first decryption limitation;~~

~~a decryption limitation updating section for updating the first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule;~~

~~a contents key generation section within the decryption device for generating the contents decryption key from the second decryption limitation; and~~

~~a first decryption section for decrypting encrypted contents transferred from the encryption device using the contents decryption key generated by the contents key generation section~~

a second contents key generation section for generating the contents decryption key from a second decryption limitation, the second decryption limitation obtained by updating a first decryption limitation in the decryption device;

a first decryption section for decrypting an encrypted contents transferred from the encryption device using the contents decryption key generated by the second contents key generation section;

a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule;

a second encryption section for encrypting the second decryption limitation using a time-varying key, and outputting a first encrypted decryption limitation; and,

a third decryption section for decrypting a second encrypted decryption limitation transferred from a third encryption section using the time-varying key and outputting the first decryption limitation;

wherein cryptographic communication is performed between the encryption device and the decryption device using a contents encryption key and the contents decryption key,

wherein the encryption device includes:

a contents storage section for storing contents,

a first contents key generation section for generating the contents encryption key based on the second decryption limitation obtained by updating the first decryption limitation, and

a first encryption section for encrypting the contents using the contents encryption key and outputting the encrypted contents, and

the third encryption section for encrypting the first decryption limitation using a time-varying key and outputting the second encrypted decryption limitation to the decryption device;

a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation,

wherein the time-varying key is not required to be transmitted to the decryption device; and

wherein the first contents key generation section generates the contents encryption key based on the second decryption limitation generated by the second decryption section.

27. (Cancelled)

28. (previously presented) A decryption device according to claim 26, further including

a common key storage section for storing a common key,

a random number generation section for generating a second random number,

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, and

a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section.

29. (Cancelled)

30. (Cancelled)

31. (original) A decryption device according to claim 28, wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

32. (previously presented) A decryption device according to claim 28, wherein the contents key generation section generates the contents decryption key based on the second decryption limitation and the time-varying key.

33. (original) A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

34. (original) A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

35. (previously presented) A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section generates the contents decryption key based on the second decryption limitation and the data sequence key.

36. (previously presented) A decryption device according to claim 28, further including a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section generates the contents decryption key based on the second decryption limitation, the time-varying key, and the data sequence key.

37. (Currently Amended) A recording medium storing a program for use in causing a computer to perform cryptographic communication ~~with an encryption device using a contents decryption key~~, wherein:

the program causes the computer to function as:

~~a second decryption section for decrypting a second~~ first ~~encrypted decryption limitation transferred from the encryption device using a time-varying key and outputting a first decryption limitation;~~

~~a decryption limitation updating section for updating the first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule;~~

~~a contents key generation section for generating the contents decryption key from the second decryption limitation; and~~

~~a first decryption section for decrypting encrypted contents transferred from the encryption device using the contents decryption key generated by the contents key generation section~~

an encryption device and a decryption device, wherein cryptographic communication is performed between the encryption device and the decryption device using a contents encryption key and a contents decryption key,

wherein the encryption device includes

a contents storage section for storing contents,

a first contents key generation section for generating the contents encryption key based on a second decryption limitation obtained by updating a first decryption limitation, and

a first encryption section for encrypting the contents using the contents encryption key and outputting the encrypted contents, and

wherein the decryption device includes

a second contents key generation section for generating the contents decryption key from the second decryption limitation, the second decryption limitation obtained by updating the first decryption limitation in the decryption device, and

a first decryption section for decrypting the encrypted contents transferred from the encryption device using the contents decryption key generated by the second contents key generation section, and

wherein the encryption device further includes a third encryption section for encrypting the first decryption limitation using a time-varying key and outputting a second encrypted decryption limitation to the decryption device, and the decryption device further includes a third decryption section for decrypting the second encrypted

decryption limitation transferred from the third encryption section using the time-varying key and outputting the first decryption limitation, and

wherein the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and

a second encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation, and

the encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation,

wherein the time-varying key is not required to be transmitted to the decryption device; and

wherein the first contents key generation section generates the contents encryption key based on the second decryption limitation generated by the second decryption section.

38. (Cancelled)

39. (previously presented) A recording medium according to claim 37, wherein the program causes the computer to further function as:

a common key storage section for storing a common key;

a random number generation section for generating a second random number;

a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number; and

a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section.

40. (Cancelled)

41. (Cancelled)

42. (original) A recording medium according to claim 39, wherein the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

43. (previously presented) A recording medium according to claim 39, wherein the contents key generation section generates the contents decryption key based on the second decryption limitation and the time-varying key.

44. (original) A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

45. (original) A recording medium according to claim 39, wherein:

the program causes the computer to further function as a sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

46. (previously presented) A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the contents key generation section generates the contents decryption key based on the second decryption limitation and the data sequence key.

47. (previously presented) A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device; and

the contents key generation section generates the contents decryption key based on the second decryption limitation, the time-varying key, and the data sequence key.

48. (previously presented) A copyright protection system according to claim 1, wherein the first and second contents key generation sections generate the contents encryption key and the contents decryption key by using an algorithm which uses the second decryption limitation as an input.

49. (previously presented) A copyright protection system according to claim 48, wherein the algorithm is a one-way function.

50. (previously presented) A copyright protection system according to claim 1, wherein neither the contents encryption key nor the contents decryption key is required to be transmitted between the encryption device and the decryption device, and wherein the time-varying key is not required to be transmitted between the encryption device and the decryption device.

3. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.

4. Claims 1, 3-14, 16-26, 28, 31-37, 39, 42-50 now re-numbered as claims 1-42 are pending.

Response to Arguments

5. Applicant's arguments in the action filed 11/17/2008, has been found persuasive in light of the limitations of the amended claims, and discussions during the telephone interview conducted 2/25/2009 (please see the attached Interview Summary).

Allowable Subject Matter

6. Amended claims 1, 3-14, 16-26, 28, 31-37, 39, 42-50, now re-numbered as claims 1-42 are allowed.

Conclusion

7. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571

272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Farid Homayounmehr Examiner
Art Unit 2439

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434